Minister of Innovation, Science and Industry
Ministre de l'Innovation, des Sciences et de l'Industrie

☐ Secret ☐ Urgent	Correspondence/Correspondance	Docket No. / Nº du chemise **0324854**

Lead / Secteur	Rec. date / Date reçue	Issue / Sujet	
SIPS	**2020-01-13**		
Due / Date d'échéance	Doc. Date / Date dos.	File No. / Nº de dossier	☐ X-ref.
2020-01-28	**2020-01-10**		

Task / Tâche

☒ Draft Reply
Projet de réponse

☐ Information
Information

☐ Meeting/Réunion ☐ Invitation

Location: _____

Date: _____

☐ Recommendation
Recommandation

☐ MIN Decision
Décision MIN

Copies ☐ _____

#: ☐ _____

☐ Transfer/Transfert:
_____

☐ _____

Portfolio ☐ _____

Date	Referred to Envoyée à	Referred by Envoyée par	Remarks Remarques	Initials Initiales

Analyst / Analyste:

Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada

Deputy Minister
Sous-ministre

Ottawa, Canada
K1A 0H5

Security classification: PROTECTED	
CCM Number: BN0004506	
Lead Sector: SIPS	Consulted: n/a
Contact: Jennifer Miller, SIPS, MFPB, 343-291-2133	
Originator: Barbara Dourley, SIPS, MFPB	
Action Required: For signature by the Minister at his earliest convenience	

ADVICE TO THE MINISTER OF INNOVATION, SCIENCE AND INDUSTRY

Privacy Commissioner of Canada Letter to the Minister on PIPEDA Modernization and Office of the Privacy Commissioner Consultation on Artificial Intelligence

SUMMARY

- On January 10, 2020, the Privacy Commissioner of Canada wrote to the Minister to congratulate him on his recent re-election and appointment as Minister of Innovation, Science and Industry. The letter, attached as "Annex A," also enumerated the Commissioner's recommendations for modernization of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

- On January 28, 2020, the Office of the Privacy Commissioner (OPC) launched a "Consultation on artificial intelligence" to solicit comments on its proposals for PIPEDA and broader privacy law reform with respect to artificial intelligence (AI).

- It is recommended that the Minister sign the letter replying to the Commissioner's letter of congratulation and regarding PIPEDA reform, attached as "Annex B". It is further recommended that I meet with the Commissioner to discuss the Commissioner's recent recommendations for PIPEDA modernization and the OPC consultation on AI.

BACKGROUND

On January 10, 2020, the Privacy Commissioner of Canada, Daniel Therrien, wrote to Minister Bains to congratulate him on his recent re-election and appointment as Minister of Innovation, Science and Industry. The Commissioner's letter also enumerated recommendations for the modernization of PIPEDA. The letter reiterated the recommendations made by the Commissioner in his 2018-2019 Annual Report to Parliament

on the *Privacy Act* and PIPEDA, which was tabled in Parliament on December 10, 2019. In particular, the Commissioner underlined his recommendations to redraft PIPEDA as a human rights-based law and to strengthen the enforcement powers of the OPC through order-making powers and administrative monetary penalties (AMPs).

On January 28, 2020, the OPC launched a "Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence," as a subset of its policy analysis work on legislative reform of privacy laws in Canada. The consultation paper, attached as "Annex C," includes several recommendations for amendments to PIPEDA with respect to AI and also further reiterates recommendations from the Commissioner's letter to the Minister and his Annual Report.

On January 27, 2020, the Commissioner wrote to Dr. Foteini Agrafioti and Dr. Yoshua Bengio, co-chairs of the Advisory Council on Artificial Intelligence, to advise them of the OPC consultation on AI and to request a meeting with the Council to discuss the consultation paper. Innovation, Science and Economic Development (ISED) officials supporting the AI council secretariat are working with the co-chairs to respond to the Commissioner's request, and will brief your office on the proposed approach.

CONSIDERATIONS

The May 21, 2019 ISED discussion paper outlining proposals for modernizing PIPEDA addresses some of the recommendations made by the Commissioner in his recent letter to the Minister. Included in the paper are proposals for expanding upon and clarifying existing rights under PIPEDA, such as a right to data mobility and a right to deletion, and for strengthening the enforcement and oversight of PIPEDA. With respect to AI, the discussion paper proposes to increase transparency around the use of automated decision-making systems where decisions may be impactful to individuals.

The Minister's mandate letter further highlighted these proposals as priorities and instructed the Minister to "Work with the Minister of Justice and Attorney General of Canada and the Minister of Canadian Heritage to advance Canada's Digital Charter and enhanced powers for the Privacy Commissioner, in order to establish a new set of online rights".

[redacted] Section 7 (Life, liberty and security of person) and Section 8 of the *Charter*

s.21(1)(a)
s.21(1)(b)
s.23

(protection against unreasonable search and seizure) are largely acknowledged as the "right to privacy" in Canada. In addition, the Supreme Court of Canada has identified the *Privacy Act* as quasi-constitutional. However, the *Privacy Act* has its origins in the *Canadian Human Rights Act.* PIPEDA is a separate piece of legislation whose purpose is to balance privacy interests against the needs to use personal information for commercial activities.

ISED officials in the Marketplace Frameworks Policy Branch are continuing work on the development of options for legislative reform to implement the Digital Charter. This includes closely examining the legal and policy implications of the Commissioner's recommendations. In particular ISED officials have [redacted]

RECOMMENDATION

It is recommended that the Minister sign the attached letter, attached as "Annex B," which thanks the Commissioner for his letter of congratulation and acknowledges receipt of his recommendations on PIPEDA modernization. It is further recommended that I meet with the Commissioner to discuss the Commissioner's most recent recommendations for PIPEDA modernization and the OPC consultation on AI.

Simon Kennedy

_____ I approve

_____ I do not approve

Attachments

Commissaire à la protection de la vie privée du Canada
Privacy Commissioner of Canada

10 JAN. 2020

L'honorable Navdeep Bains, C.P., député
Ministre de l'Innovation, des Sciences et de l'Industrie
Édifice C.D. Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5

Monsieur le Ministre,

Je tiens à vous féliciter pour votre récente réélection et le renouvellement de votre mandat à titre de ministre de l'Innovation, des Sciences et de l'Industrie. Votre ministère et le Commissariat collaborent depuis longtemps sur les questions de protection de la vie privée dans le secteur privé, et je me réjouis à la perspective de poursuivre cette coopération.

J'ai trouvé encourageant de constater l'importance que le gouvernement a accordée aux droits de la personne, à la démocratie et au respect du droit international dans le discours du Trône, ainsi que son engagement à revoir les règles régissant actuellement l'environnement numérique. Ces engagements sont cohérents avec les récentes positions du Commissariat, selon lesquelles les lois canadiennes sur la protection des renseignements personnels doivent être modernisées pour reconnaître la vie privée comme étant une valeur fondamentale de la société canadienne, un droit de la personne et, comme le scandale Cambridge Analytica nous a permis de le constater, une condition nécessaire pour l'exercice d'autres droits, notamment la liberté, l'égalité et la démocratie.

Pour le meilleur et pour le pire, les technologies axées sur les données sont une force perturbatrice. Elles procurent de grands avantages aux particuliers et ouvrent la voie à l'innovation et à la croissance économique, mais elles se sont aussi révélées préjudiciables pour les droits. Avec l'avènement de ces nouvelles technologies, nous avons constaté l'essor de modèles d'affaires axés sur la surveillance qui reposent sur la collecte et le partage de données massifs et omniprésents, le profilage, la prise de décision automatisée et l'analytique comportementale. En raison de ces pratiques et de l'absence d'une législation appropriée, les gens sont incapables de participer librement à la société numérique moderne, de vivre et de s'épanouir de façon autonome, sans se livrer au regard scrutateur d'entreprises commerciales et, éventuellement, de l'État.

...2

Cette situation a donné lieu à une crise de confiance. Les Canadiens veulent profiter des avantages des technologies numériques, mais de façon sécuritaire. À l'heure actuelle, seulement 38 % des Canadiens croient que les entreprises respectent leur droit à la vie privée. Selon les conclusions de nos enquêtes, la loi n'est pas respectée dans les deux tiers des plaintes que le Commissariat reçoit concernant la loi sur la protection des renseignements personnels applicable au secteur privé. Cela est inadmissible.

Pour restaurer la confiance, la législation doit faire l'objet d'une réforme fondamentale, et non marginale. Nous devons passer du modèle actuel axé sur l'autoréglementation à une réglementation étatique qui protège les droits individuels. L'adoption d'une législation fondée sur le respect des droits, appuyée par des mécanismes de contrôle efficaces, favoriserait l'innovation responsable et renforcerait la confiance envers le gouvernement et les entreprises. Cela permettrait aux gens de participer pleinement et en toute confiance à l'économie numérique.

Le Commissariat a récemment étudié la question de l'adoption d'une approche fondée sur les droits dans nos lois sur la protection de la vie privée. Un chapitre de mon récent rapport annuel 2018-2019 au Parlement, déposé le 10 décembre 2019, traite de propositions concrètes à cet égard. Pour enchâsser la protection de la vie privée dans le cadre qui lui est propre, soit celui des droits de la personne, la législation devrait être rédigée de sorte que le droit à la protection de la vie privée soit interprété et appliqué selon ses valeurs sous-jacentes, comme un droit de la personne et un élément essentiel à l'exercice d'autres droits fondamentaux. À cette fin, notre rapport suggère l'adoption d'un préambule et d'une clause d'objet qui définissent ces valeurs, tout en reconnaissant l'intérêt légitime des organisations commerciales et l'intérêt public.

Vous trouverez à la fin de la présente un modèle de préambule et d'énoncé d'objet qui pourraient être ajoutés à la LPRPDE. J'espère que vous conviendrez que ces dispositions interprétatives, qui reflètent les valeurs canadiennes et qui sont susceptibles d'améliorer la confiance, n'entraveraient pas l'innovation responsable. Nos propositions appuient également l'innovation en suggérant de nouvelles exceptions relatives au consentement lorsque ce principe n'est pas efficace pour protéger la vie privée, comme dans certaines situations mettant en jeu l'intelligence artificielle.

Dans le rapport, j'ai proposé quatre éléments clés qu'une loi fondée sur les droits devrait contenir. Premièrement, la loi devrait comprendre une définition de la vie privée au sens large, reconnaissant son ampleur et sa portée, non pas comme un ensemble de règles liées au processus comme le consentement, l'accès et la transparence, mais comme un droit de la personne. La protection de la vie privée est souvent considérée à travers le prisme des politiques de confidentialité des sites Web menant à une forme imparfaite du consentement. Il s'agit d'un point de vue réducteur qui défavorise nettement les individus lorsqu'ils sont confrontés à des organisations ayant infiniment plus de pouvoir.

...3

Deuxièmement, nos lois sur la protection des renseignements personnels devraient reconnaître la nature quasi constitutionnelle des lois relatives à la vie privée. Cela signifie qu'il faut confirmer le statut particulier de la protection de la vie privée et reconnaître le rôle fondamental qu'elle joue dans la préservation d'une société libre et démocratique.

Troisièmement, la loi devrait être rédigée comme un texte législatif habituel, conférant des droits et imposant des obligations. Ainsi, la LPRPDE ne devrait plus être rédigée comme un code de conduite de l'industrie, assorti de quelques obligations, mais aussi de plusieurs recommandations, exemples et bonnes pratiques qui ne créent pas de droits exécutoires pour les personnes. Nous avons vu dans l'affaire Facebook comment les recommandations n'offrent pas une protection réelle.

Quatrièmement, la loi doit prévoir des mécanismes de contrôle qui offrent des recours rapides et efficaces aux personnes dont le droit à la vie privée n'a pas été respecté, et qui contribuent à assurer la conformité continue des organisations. Cela comprend l'habilitation du commissaire à la protection de la vie privée à rendre des ordonnances exécutoires et à imposer des sanctions administratives pécuniaires en cas de non-respect de la loi. De plus, le Commissariat devrait être en mesure de mener des inspections proactives pour s'assurer que les organisations sont manifestement responsables de leurs pratiques en matière de protection de la vie privée. Ces pouvoirs accrus, qui seraient bien sûr exercés conformément aux règles traditionnelles de justice naturelle et sous réserve d'un contrôle judiciaire, donneraient aux Canadiens une plus grande assurance qu'ils participent à un marché numérique qui prend la vie privée au sérieux et que des sanctions conséquentes sont imposées lorsque leurs droits ont été enfreints.

En ce qui concerne les pouvoirs exécutoires, j'ai remarqué que votre lettre de mandat, celle du ministre de la Justice et procureur général ainsi que celle du ministre de Patrimoine canadien faisaient toutes mention d'un pouvoir accru pour le Commissariat. La Charte numérique du gouvernement mentionne qu'il faudrait accorder au Commissariat un pouvoir « limité » de rendre des ordonnances. Toujours selon la Charte, je devrais, après avoir mené ma propre enquête, convaincre le procureur général de faire enquête de nouveau et, à terme, de porter l'affaire devant la cour avant que des amendes ne puissent être imposées aux contrevenants. À mon avis, la proposition du gouvernement est complètement inefficace. La division des pouvoirs de contrôle entre l'organisme de réglementation et les tribunaux retarderait le moment auquel les particuliers jouiraient de leurs droits et inciterait les entreprises à ne pas prendre la protection des renseignements personnels au sérieux. Par comparaison, mes homologues européens et américains, entre autres, peuvent ordonner directement aux entreprises de se conformer à la loi et leur imposer des sanctions financières assez lourdes.

...4

Selon mes homologues provinciaux et étrangers qui ont déjà ces pouvoirs de rendre des ordonnances et d'imposer des sanctions pécuniaires, les entreprises semblent beaucoup plus disposées à collaborer avec eux depuis qu'ils ont été dotés de ces outils. Dans les cas où l'autorité de réglementation conclut qu'il y a eu manquement à la loi, les entreprises corrigent plus facilement le tir sans délai indu. Doter le commissaire fédéral à la protection de la vie privée de pouvoirs réels à cet égard contribuera à faire en sorte que les droits soient protégés et que les organisations soient tenues responsables, et ce de manière efficace et rapide.

Vous avez reçu un mandat ambitieux, qui comprend un certain nombre de réformes législatives possibles, certaines nouvelles, comme l'adoption de règlements concernant la protection des données personnelles supervisée par un commissaire aux données, et d'autres qui ont fait l'objet de discussions antérieures, comme les lois sur la propriété effective. Je serais heureux de me pencher sur ces questions avec vous et votre ministère.

Le Canada a déjà été un chef de file en matière de protection de la vie privée; il semble malheureusement que le monde a maintenant une longueur d'avance sur nous. D'innombrables administrations à l'échelle de la planète ont pris des mesures pour améliorer leurs lois en matière de protection de la vie privée afin de mieux protéger leurs citoyens. Le *Règlement général sur la protection des données* (RGPD) de l'Union européenne est l'exemple le plus notable de la modernisation législative des dernières années, ayant fait passer la notion de protection des renseignements personnels au niveau supérieur à l'échelle mondiale. Dans l'année qui vient, l'Union européenne examinera le statut du Canada en matière de protection adéquate. Il est impératif que les lois du Canada soient jugées comme offrant un niveau de protection adéquat comparativement à leurs équivalents européens. Si notre régime de protection de la vie privée est considéré comme étant inadéquat, il y aura de véritables répercussions économiques pour les entreprises canadiennes et des effets importants sur la place du Canada dans l'ensemble de l'économie numérique.

Aux États-Unis, la *California Consumer Privacy Act* (loi sur la protection de la vie privée des consommateurs de la Californie) et de récentes propositions législatives en vue d'une loi fédérale complète sur la protection des données sont le signe d'un pas s'éloignant de l'autoréglementation des entreprises, grâce à l'entrée en vigueur de droits donnant ouverture à des poursuites pour les particuliers et de sanctions pour les entreprises qui ne respectent pas la loi. Je vois difficilement pourquoi nous ne pourrions pas protéger les Canadiens d'une manière semblable et ne pas imposer des conséquences de la sorte aux entreprises canadiennes qui ne respectent pas la loi.

...5

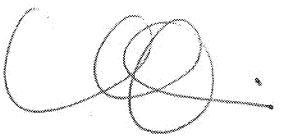
Le Canada devrait prendre des mesures sérieuses pour améliorer ses lois en matière de protection de la vie privée et pour regagner sa réputation de chef de file mondial en matière de protection des renseignements personnels. Cette démarche améliorerait non seulement la protection des droits des particuliers et favoriserait la confiance à l'égard des activités commerciales; elle favoriserait aussi l'interopérabilité entre États, ce qui accroîtrait la prévisibilité et pourrait se solder en économies pour les entreprises canadiennes.

On peut affirmer sans crainte d'exagérer que la numérisation de tant d'aspects de nos vies est en train de transformer l'humanité. Si nous ne faisons pas attention, elle prendra une forme qui ne correspond pas à nos valeurs ni à nos droits les plus fondamentaux. Par conséquent, on ne devrait pas autoriser les utilisations de la technologie qui sont incompatibles avec ces valeurs et ces droits. Le marché a prouvé à maintes reprises qu'il est créatif. Il trouvera des moyens rentables d'offrir des produits et des services qui répondent à des besoins véritables, tout en respectant un cadre législatif renouvelé qui respecte ces droits et ces valeurs.

J'anticipe avec empressement de travailler avec vous et avec le Parlement pour mettre sur pied un régime complet de protection des renseignements personnels suffisamment solide pour résister aux réalités sociales, juridiques et technologiques du 21e siècle. Je me réjouis à la perspective de poursuivre une relation fructueuse avec votre ministère au cours des années à venir. À cette fin, je serais heureux de vous rencontrer, au moment qui vous conviendra, pour discuter plus en détail de ces questions.

Je vous prie d'agréer, Monsieur le Ministre, l'expression de ma considération distinguée.

Le commissaire,



Daniel Therrien

p. j.

Préambule et énoncé d'objet proposés pour la LPRPDE

Vous trouverez ci-après un modèle de préambule et d'énoncé d'objet qui renvoient plus clairement et plus explicitement aux valeurs et aux droits fondamentaux qui devraient sous-tendre la LPRPDE. Nous recommandons qu'à la fois un préambule et un énoncé d'objet apparaissent au début de la Loi.

Préambule

ATTENDU QUE la protection de la vie privée est un droit fondamental de chaque personne et une valeur fondamentale protégée dans les instruments internationaux portant sur les droits de la personne dont le Canada est signataire;

ATTENDU QUE le droit à la vie privée protège l'autonomie et la dignité individuelles et est lié à la protection de la réputation et à la liberté de pensée et d'expression;

ATTENDU QUE la protection de la vie privée est nécessaire au maintien de relations de confiance mutuelle qui sont essentielles au tissu social canadien;

ATTENDU QUE la protection de la vie privée est essentielle à la préservation de la démocratie ainsi qu'à la pleine jouissance et à l'exercice de bon nombre des droits et libertés garantis par la *Charte canadienne des droits et libertés*;

ATTENDU QUE le contexte technologique actuel et en constante évolution facilite la collecte de quantités massives de données personnelles ainsi que l'utilisation de ces données, qu'elles soient identifiables, agrégées ou rendues anonymes, d'une manière qui peut avoir des répercussions négatives sur les personnes, les groupes et les communautés;

ATTENDU QUE le traitement des données personnelles doit être conçu pour servir l'humanité;

ATTENDU QUE le traitement responsable des données personnelles peut servir des intérêts publics tels que la croissance économique, l'amélioration des soins de santé et la protection de l'environnement;

ATTENDU QUE cette loi protège le droit à la vie privée des personnes tout en reconnaissant l'intérêt légitime des organisations à recueillir, à utiliser et à communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances et d'une manière qui ne constitue pas de la surveillance;

ATTENDU QUE le droit à la vie privée doit être mis en équilibre avec d'autres droits fondamentaux comme le droit à la liberté d'expression dans des circonstances où la collecte, l'utilisation ou la communication de renseignements personnels sert un intérêt public légitime;

ET ATTENDU QUE cette loi a été reconnue par les tribunaux comme étant de nature quasi constitutionnelle.

Objet

La présente loi a pour objet :

(a) de mettre en œuvre le droit fondamental à la vie privée des individus dans le contexte commercial au moyen d'une solide protection des données qui garantit que le traitement des données est licite, équitable, proportionnel, transparent et responsable, et respecte les droits et libertés fondamentaux de la personne;

(b) d'établir un équilibre entre le droit à la vie privée et le droit à la liberté d'expression dans des circonstances où la collecte, l'utilisation ou la communication de renseignements personnels sert un intérêt public légitime;

(c) d'établir un équilibre, le cas échéant, entre le droit à la vie privée et ce qu'exige l'intérêt public;

(d) de protéger le droit à la vie privée des personnes tout en reconnaissant l'intérêt légitime des organisations à recueillir, à utiliser et à communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances et d'une manière qui ne constitue pas de la surveillance;

(e) d'offrir aux personnes des recours rapides et efficaces lorsque leur droit à la vie privée n'est pas respecté et de veiller à ce que les organisations s'acquittent en permanence de leurs obligations prévues dans la présente Loi.

Commissaire à la protection de la vie privée du Canada
Privacy Commissioner of Canada

JAN 10 2020

The Honourable Navdeep Bains, P.C., M.P.
Minister of Innovation, Science and Industry
C.D. Howe Building
235 Queen Street
Ottawa, Ontario K1A 0H5

Dear Minister,

I am writing to offer my congratulations on your recent re-election, and on your re-appointment as Minister of Innovation, Science and Industry. Your department and my office have a long history of working together on private sector privacy issues, and I look forward to continuing this cooperation.

I was encouraged to see the prominence this government placed on human rights, democracy and respect for international law in the Speech from the Throne, as well as the commitment to review the rules currently in place for the digital environment. These commitments are in line with recent positions put forth by my office that Canada's privacy laws need to be updated to recognize privacy as a foundational value in Canadian society, a human right and, as we have seen in the recent Cambridge Analytica scandal, a prior condition to the exercise of other rights, including freedom, equality and democracy.

For good and bad, data-driven technologies are a disruptive force. While they bring great benefits for individuals and open the door to innovation and economic growth, they have too often been shown to be harmful to rights. With the advent of new technologies, we have seen the rise of surveillance based business models, which are predicated on ubiquitous and mass data collection and sharing, profiling, automated decision-making and behavioural data analytics. As a result of these practices and in the absence of adequate laws, individuals are unable to freely participate in a modern digital society, to live and develop independently as persons, away from the watchful eye of commercial enterprises and, eventually, government.

This has resulted in a crisis of trust. Canadians want to enjoy the benefits of digital technologies, but they want to do it safely. Right now, only 38% of Canadians believe businesses respect their privacy rights. In two-thirds of the complaints my Office receives under our private-sector privacy law, we find that the law is not respected. This is untenable.

.../2

30, rue Victoria, 1er étage | 30 Victoria Street, 1st Floor
Gatineau (Québec) K1A 1H3
Sans frais/Toll free 1-800-282-1376 Tél./Tel: 819-994-5444 Téléc./Fax: 819-994-5424 www.priv.gc.ca

To restore trust, the law must be reformed fundamentally, not marginally. We need to shift from the current self-regulatory model to state-based regulation that protects individual rights. Incorporating a rights-based framework in our privacy laws, along with effective enforcement mechanisms, would provide the necessary conditions to allow for responsible innovation and foster trust in government and business, giving individuals the confidence to fully participate in the digital age.

My Office has recently examined how to best incorporate a human rights-based approach into our privacy laws. A chapter in my recent 2018-2019 Annual Report to Parliament, tabled on December 10, 2019, put forth tangible proposals in this regard. To entrench privacy in its proper human rights framework, the law should ensure that the right to privacy is interpreted and applied in relation to its underlying values, as a human right and an essential element in the exercise of other fundamental rights. To that end, our report suggests the adoption of a preamble and purpose clauses that seek to reflect these values while, importantly, acknowledging legitimate business interests and the public interest.

You will find attached at the end of this letter a model preamble and purpose statement for possible inclusion in PIPEDA. I trust you will agree that these interpretive clauses, while reflective of Canadian values and likely to improve trust, would not impede responsible innovation. Our proposals also support innovation by suggesting new exceptions to consent where that principle is not effective in protecting privacy, such as in certain situations involving artificial intelligence.

I further elaborated in the report on four key elements that a rights-based law should contain. First, the law should include a broad definition of privacy, recognizing its proper breadth and scope, not as a set of process rules like consent, access and transparency, but as a human right. Privacy is often seen through the lens of website terms and conditions leading to a less than meaningful form of consent. This is a narrow view, and one that puts individuals at a distinct disadvantage when faced with organizations with immeasurably more power.

Second, our privacy laws should recognize the quasi-constitutional nature of privacy legislation. This means confirming the protected status of privacy and the fundamental role it plays in the preservation of a free and democratic society.

Third, the law should be drafted in the usual manner of legislation, conferring rights and imposing obligations. This means PIPEDA should no longer be drafted as an industry code of conduct, with some obligations but also several recommendations, examples and good practices that do not create enforceable entitlements for individuals. We have seen in the Facebook matter how recommendations do not offer meaningful protection.

.../3

Fourth, the law must provide for enforcement mechanisms that offer quick, effective remedies for people whose privacy rights were not respected, and that help to ensure ongoing compliance by organizations. This includes empowering the Privacy Commissioner to make binding orders and impose administrative monetary penalties ("AMPS") for non-compliance with the law. As well, my office should be enabled to conduct proactive inspections to ensure organizations are demonstrably accountable for their privacy practices. These enhanced powers, which of course would be exercised in accordance with traditional rules of natural justice and subject to judicial review, would give Canadians greater assurances to participate in a digital marketplace that takes privacy seriously and imposes meaningful sanctions when rights have been violated.

On the issue of enforcement powers, I note that both your mandate letter, the letter for the Minister of Justice and Attorney General, and the letter for the Minister of Canadian Heritage referenced enhanced powers for my Office. I further note that the government's Digital Charter suggests that my Office should be granted "circumscribed" order-making powers and that before fines are imposed for violations of the law that I have identified following an investigation, I should first convince the Attorney General to further investigate and eventually bring the matter before a judge. In my view, this proposal would be very inefficient, as splitting powers between the regulator and the courts would delay the enjoyment of rights by individuals and create incentives for companies to not take privacy seriously. By contrast, my EU and US equivalents, among others, can directly order companies to comply with the law and issue sizeable administrative penalties.

I would also note that my fellow privacy commissioners at both the provincial and international levels who have already been empowered to make orders and impose financial penalties report that these enforcement tools have led to much more cooperation from companies. When the regulator finds a violation, companies are more willing to correct deficiencies, without long delays. Equipping the federal privacy commissioner with meaningful powers in this regard will help ensure that rights are protected and organizations are held accountable, in a quick and effective way.

You have been given an ambitious mandate, one that includes a number of possible legislative reforms, some new, such as the adoption of regulations involving the protection of personal data overseen by a Data Commissioner, and others that have been the subject of previous discussions, such as legislation on beneficial ownership. I would welcome engagement with you and your department on these issues.

.../4

While Canada used to be a leader in privacy protection, unfortunately the world is now passing us by. Countless jurisdictions worldwide have taken steps to enhance their privacy laws to better protect their citizens. The EU *General Data Protection Regulation* is the most notable example of legislative modernization in recent years that has raised the "privacy bar" worldwide. As we approach the review of Canada's adequacy status with the European Union in the next year, it is imperative that Canada's laws are assessed as providing an adequate level of protection when compared to those of our European counterparts. If our privacy regime is found to not be adequate, there will be real economic impacts for Canadian businesses and profound effects for Canada's place in the digital economy writ large.

In the United States, the *California Consumer Privacy Act* and recent legislative proposals for a comprehensive federal data privacy law all signal a move away from corporate self-regulation, containing actionable rights for individuals and penalties for companies that fail to adhere to the law. It is unclear why Canadians would not have similar protections of their rights and Canadian businesses not face similar consequences for failing to comply with the law.

Canada should take meaningful action to enhance its privacy laws and gain back its reputation as a global privacy leader. This would have the benefit of not only enhancing protection of individuals' rights and promoting trust in commercial activities but it would also help promote interoperability between jurisdictions, providing predictability and potential cost savings to Canadian businesses.

It is not an exaggeration to say that the digitization of so much of our lives is reshaping humanity. If we are not careful, it will be reshaped in ways that do not accord with our most fundamental rights and values. Therefore, uses of technology that are incompatible with these rights and values should not be permitted. The market has proven time and again that it is creative; it will find profitable ways to offer products and services that meet genuine needs while respecting new laws that are based on rights and values.

I look forward to working with you and Parliament to create a more comprehensive privacy protection regime that is fundamentally robust enough to withstand the social, legal and technological realities of the 21st century. I also welcome a continued positive relationship with your department in the years to come. To that end, I would be happy to meet with you at your convenience to discuss these matters further.

Sincerely,

Daniel Therrien
Commissioner

Encl.

Proposed preamble and purpose clause for PIPEDA

What follows is a model preamble and purpose statement that would provide clearer and more explicit reference to the fundamental rights and values that should underlie PIPEDA. We recommend that both a preamble and a purpose statement appear at the opening of the Act.

Preamble

WHEREAS privacy is a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada is a signatory;

WHEREAS the right to privacy protects individual autonomy and dignity, and is linked to the protection of reputation and freedom of thought and expression;

WHEREAS privacy is essential to relations of mutual trust and confidence that are fundamental to the Canadian social fabric;

WHEREAS privacy is essential to the preservation of democracy and the full and meaningful enjoyment and exercise of many of the rights and freedoms guaranteed by the *Canadian Charter of Rights and Freedoms*;

WHEREAS the current and evolving technological context facilitates the collection of massive quantities of personal data as well as the use of these data, whether in identifiable, aggregate or anonymized forms, in ways that can adversely impact individuals, groups and communities;

WHEREAS the processing of personal data should be designed to serve humankind;

WHEREAS responsible processing of personal data can serve public interests such as economic growth, advances in health care and the protection of the environment;

WHEREAS this law protects the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances and in ways that do not represent surveillance;

WHEREAS the right to privacy must be balanced with other fundamental rights such as the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

AND WHEREAS this statute has been recognized by the courts as being quasi-constitutional in nature;

Purpose

The purposes of this Act are:

(a) to implement the fundamental right to privacy of all persons in the commercial context through robust data protection that ensures that the processing of data is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and freedoms of individuals;

(b) to balance privacy rights with the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

(c) to balance privacy rights, where appropriate, with what the public interest requires;

(d) to protect the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances and in ways that do not represent surveillance;

(e) to provide individuals with quick and effective remedies when their privacy rights have not been respected and to ensure the ongoing compliance by organizations with their obligations under this Act.

Minister of Innovation, Science and Industry

Ministre de l'Innovation, des Sciences et de l'Industrie

To: Mr. Daniel Therrien
Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, QC, K1A 1H3

Dear Commissioner Therrien:

Thank you for your letter of January 10, 2020 regarding modernization of the *Personal Information Protection and Electronic Documents Act* and for your words of congratulation on my appointment as Minister of Innovation, Science and Industry. I am pleased to be returning to Innovation, Science and Economic Development Canada, and I look forward to continued cooperation between our organizations.

I have taken note of the recommendations for modernization of PIPEDA outlined in your letter, including incorporating a rights-based framework into the law, recognizing the broad scope of privacy and its protected status, redrafting PIPEDA in the usual manner of legislation, and providing for enforcement mechanisms that offer quick, effective remedies for people whose privacy rights have not been respected. My officials are closely examining the legal and policy implications of the recommendations outlined in your letter.

As you know, on May 21, 2019, I announced Canada's Digital Charter, which lays the foundation for modernizing the rules that govern the digital sphere in Canada and for rebuilding Canadians' trust in the digital economy. Accompanying the launch of the Digital Charter, the Government also announced a set of actions that will serve to implement the Charter's principles, highlighted by proposals to modernize PIPEDA and enhance enforcement and oversight of the Act. As per the direction provided to me by the Prime Minister in my mandate letter of December 13, 2019, my department is currently examining options to move forward with these commitments. We are fully committed to ensuring that Canada maintains a comprehensive privacy regime.

Moving forward, and following your meeting of October 10, 2019, my Deputy Minister, Simon Kennedy, would be happy to meet with you to continue this discussion. Please have your officials get in touch at your convenience.

Sincerely,

The Honourable Navdeep Bains, P.C., M.P.

Canada

Minister of Innovation, Science and Industry

Ministre de l'Innovation, des Sciences et de l'Industrie

À : M. Daniel Therrien
Commissaire à la protection de la vie privée du Canada
30, rue Victoria, 1er étage
Gatineau (Québec) K1A 1H3

Monsieur le commissaire Therrien,

Je vous remercie de votre lettre du 10 janvier 2020 au sujet de la modernisation de la *Loi sur la protection des renseignements personnels et les documents électroniques* et de vos félicitations pour ma nomination au poste de ministre de l'Innovation, des Sciences et de l'Industrie. Je suis heureux de revenir à Innovation, Sciences et Développement économique Canada et je me réjouis à la perspective de voir nos organisations continuer à collaborer.

J'ai pris note des recommandations que vous formulez dans votre lettre en vue de moderniser la LPRPDE, dont celles d'intégrer dans la loi un cadre fondé sur les droits, de reconnaître la vie privée au sens large et d'en assurer la protection, de reformuler la LPRPDE de la manière habituelle pour une loi et de prévoir des mécanismes d'application qui offrent des recours rapides et efficaces aux personnes dont les droits à la vie privée ont été enfreints. Mes fonctionnaires examinent de près les incidences juridiques et politiques des recommandations que vous présentez dans votre lettre.

Comme vous le savez, le 21 mai 2019, j'ai annoncé la Charte canadienne du numérique, qui représente le point d'ancrage pour moderniser la réglementation de l'univers du numérique au Canada et pour rétablir la confiance des Canadiens dans l'économie numérique. Ce lancement par le gouvernement de la Charte canadienne du numérique s'accompagnait d'un ensemble de mesures visant à mettre en œuvre les principes de la Charte, notamment des propositions ayant pour but de moderniser la LPRPDE et de renforcer l'application et la surveillance de la Loi. Conformément à l'orientation que m'a donnée le premier ministre dans ma lettre de mandat du 13 décembre 2019, mon ministère est à examiner des moyens de donner suite à ces engagements. Nous avons la ferme intention d'assurer au Canada le maintien d'un régime complet de protection de la vie privée.

Dans la foulée de votre réunion du 10 octobre 2019, mon sous-ministre, Simon Kennedy, sera heureux de vous rencontrer afin de poursuivre cette discussion. Veuillez demander à vos fonctionnaires de communiquer avec nous au moment qui vous conviendra.

Je vous prie d'agréer, Monsieur Therrien, mes salutations distinguées,

Canada

L’honorable Navdeep Bains, C.P., député

Consultation on the OPC (Office of the Privacy Commissioner of Canada)'s Proposals for ensuring appropriate regulation of artificial intelligence

Seeking views on the OPC (Office of the Privacy Commissioner of Canada)'s recommendations to Government/Parliament

Introduction

The Office of the Privacy Commissioner of Canada (OPC) is currently engaged in legislative reform policy analysis of both federal privacy laws. We are examining artificial intelligence (AI) as a subset of this work as it relates specifically to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). We are of the view that PIPEDA (Personal Information Protection and Electronic Documents Act) falls short in its application to AI (artificial intelligence) systems and we have identified several areas where PIPEDA (Personal Information Protection and Electronic Documents Act) could be enhanced. We are seeking to consult with experts in the field to validate our understanding of how privacy principles should apply and whether our proposals would be consistent with the responsible development and deployment of these systems.

We are paying specific attention to AI (artificial intelligence) systems given their rapid adoption for processing and analysing large amounts of personal information. Their use for making predictions and decisions affecting individuals may introduce privacy risks as well as unlawful bias and discrimination.

It is clear that AI (artificial intelligence) provides for many beneficial uses. For example, AI (artificial intelligence) has great potential in improving public and private services, and has helped spur new advances in the medical and energy sectors among others. However, the impacts to privacy, data protection and, by extension, human rights will be immense if clear rules are not enshrined in legislation that protect these rights against the possible negative outcomes of AI (artificial intelligence) and machine learning processes.

The June 2019 G20 Ministerial Statement on Trade and Digital Economy committed to a human-centered approach to AI (artificial intelligence), recognizing the need to continue to promote the protection of privacy and personal data consistent with applicable frameworks. [1](#fn1) As well, a 2019 report by Deloitte cautions that "business and government may not have much time to act to address the perceived risks of AI (artificial intelligence) before Canadians definitively turn against the new technology." [2](#fn2)

Based on our own assessment, AI (artificial intelligence) presents fundamental challenges to all foundational privacy principles as formulated in PIPEDA (Personal Information Protection and Electronic Documents Act). For instance, the data protection principle of limiting collection may be incompatible with the basic functionality of AI (artificial intelligence) systems. Some have pointed out that AI (artificial intelligence) systems generally rely on large amounts of personal data to train and test algorithms, alleging that limiting some or any of the data could lead to reduced quality and utility of the output. [3](#fn3)

As for another example, some have observed that organizations relying on AI (artificial intelligence) for advanced data analytics or consequential decisions may not necessarily know ahead of time how the information processed by AI (artificial intelligence) systems will be used or what insights they will discover. [4](#fn4) This has led some to call into question the practicality of the purpose specification principle, that requires on the one hand "specifying purposes" to individuals at the time of collecting their information and, on the other, "limiting use and disclosure" of personal information to the purpose for which it was first collected. [5](#fn5)

To echo the words of the late Ian Kerr, former Canada Research Chair in Ethics, Law, and Technology, and former member of Canada's Advisory Council on Artificial Intelligence, "we stand on the precipice of a society that increasingly interacts with machines, many of which will be more akin to agents than mere mechanical devices. If so, our laws need to reflect this stunning new reality." [6](#fn6)

To this end, we have developed what we believe to be key proposals for how PIPEDA (Personal Information Protection and Electronic Documents Act) could be reformed in order to bolster privacy protection and achieve responsible innovation in a digital era involving AI (artificial intelligence) systems. In our view, responsible innovation involving AI (artificial intelligence) systems must take place in a regulatory environment that respects fundamental rights and creates the conditions for trust in the digital economy to flourish.

We view our proposals as being interconnected and meant to be adopted as a suite within the law. To facilitate a robust discussion with experts on these matters, we pose a number of questions to elicit feedback on our suggested enhancements to PIPEDA (Personal Information Protection and Electronic Documents Act). We welcome any additional feedback experts would like to share to help shape our work in this regard.

Proposals for Consideration

Proposal 1: Incorporate a definition of AI (artificial intelligence) within the law that would serve to clarify which legal rules would apply only to it, while other rules would apply to all processing, including AI (artificial intelligence)

PIPEDA (Personal Information Protection and Electronic Documents Act) is technologically neutral and is a law of general application. As such, it does not include definitions relating to AI (artificial intelligence), automated decision-making or automated processing. However, as suggested in other proposals found in this document, there may be a need for specific rules to cover certain uses of AI (artificial intelligence), which would support defining it within the act to clarify when such rules would apply.

The OECD (Organisation for Economic Co-operation and Development) *Principles on Artificial Intelligence*, adopted in May 2019 by forty-two countries, including Canada, defines an AI (artificial intelligence) system as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI (artificial intelligence) systems are designed to operate with varying levels of autonomy." [7](#fn7) However, the Institute of Electrical and Electronics Engineers' (IEEE) *Global Initiative on Ethics of Autonomous and Intelligence Systems* takes the view that the term AI (artificial intelligence) is too vague and uses instead "autonomous and intelligent systems." [8](#fn8)

The EU (European Union)'s General Data Protection Regulation (GDPR) explicitly addresses AI (artificial intelligence) by referring to automated decision-making and profiling in Article 22. In its 2017 guidance, *Big data, artificial intelligence, machine learning and data protection*, the UK (United Kingdom) Information Commissioner's Office (ICO) distinguishes

between the key terms of AI (artificial intelligence), machine learning and big data analytics, noting they are often used interchangeably but have subtle differences. [9](#fn9) For example, the ICO (Information Commissioner's Office) refers to AI (artificial intelligence) as a key to unlocking the value of big data, machine learning as one of the technical mechanisms that facilitates AI (artificial intelligence), and big data analytics as the sum of both AI (artificial intelligence) and machine learning processes.

Discussion questions:

1. Should AI (artificial intelligence) be governed by the same rules as other forms of processing, potentially enhanced as recommended in this paper (which means there would be no need for a definition and the principles of technological neutrality would be preserved) or should certain rules be limited to AI (artificial intelligence) due to its specific risks to privacy and, consequently, to other human rights?
2. If certain rules should apply to AI (artificial intelligence) only, how should AI (artificial intelligence) be defined in the law to help clarify the application of such rules?

Proposal 2: Adopt a rights-based approach in the law, whereby data protection principles are implemented as a means to protect a broader right to privacy—recognized as a fundamental human right and as foundational to the exercise of other human rights

Paul Nemitz, Principal Adviser on Justice Policy at the EU (European Union) Commission, aptly captures why AI (artificial intelligence) requires special legal attention and the significance of checking against human rights in the rule of law:

> *AI (artificial intelligence) will in many areas of life decide or prepare decisions or choices which previously were made by humans, according to certain rules. If thus AI (artificial intelligence) now incorporates the rules according to which we live and executes them, we will need to get used to the fact that AI (artificial intelligence) must always be treated like the law itself. And for a law, it is normal to be checked against higher law, and against the basic tenants of constitutional democracy. The test every law must go through is whether it is in line with fundamental rights, whether it is not in contradiction with the principle of democracy, thus in particular whether it has been adopted in a legitimate procedure, and whether it complies with the principle of the rule of law, thus is not in contradiction to other pre-existing law, sufficiently clear and proportional to the purpose pursued.* [10](#fn10)

The purpose of the law ought to be to protect privacy in the broadest sense, understood as a human right in and of itself, and as foundational to the exercise of other human rights. This human rights based approach is consistent with the recent 2019 Resolution of Canada's Federal, Provincial and Territorial Information and Privacy Commissioners, which notes that AI (artificial intelligence) and machine learning technologies must be "designed, developed and used in respect of fundamental human rights, by ensuring protection of privacy principles such as transparency, accountability, and fairness." [11](#fn11)

Likewise, the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) resolution on AI (artificial intelligence) (2018) affirms that "any creation, development and use of artificial intelligence systems shall fully respect human rights, particularly the rights to the protection of personal data and to privacy, as well as human dignity, non-discrimination and fundamental values." [12](#fn12) The ICDPPC (International Conference of Data Protection and Privacy Commissioners)'s recent *Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising*

Other Fundamental Rights (2019) reaffirms a strong commitment to privacy as a right and value in itself, and calls for appropriate legal protections to prevent privacy breaches and impacts to human rights given advancements of new technologies like AI (artificial intelligence). [13](#fn13)

In order to ensure the protection of rights, we are of the view that PIPEDA (Personal Information Protection and Electronic Documents Act) should be given a rights-based foundation that recognizes privacy in its proper breadth and scope, and provides direction on how the rest of the Act's provisions should be interpreted. Such an approach would be consistent with many international instruments, including the GDPR (General Data Protection Regulation), which has incorporated a human rights-based approach to privacy within the EU (European Union)'s data protection legislation. Through recitals, the GDPR (General Data Protection Regulation) makes repeated references to fundamental rights of individuals in relation to data processing.

The need to firmly embed and clarify rights in PIPEDA (Personal Information Protection and Electronic Documents Act) is ever more pressing in a digital context where computers may make decisions for and about us with little to no human involvement.

Discussion question:

1. What challenges, if any, would be created for organizations if the law were amended to more clearly require that any development of AI (artificial intelligence) systems must first be checked against privacy, human rights and the basic tenets of constitutional democracy?

Proposal 3: Create a right in the law to object to automated decision-making and not to be subject to decisions based solely on automated processing, subject to certain exceptions

If we are to meaningfully protect privacy as a human right in a digital context involving AI (artificial intelligence) systems, one such right that needs to be considered is the ability to object to decisions made by computers and to request human intervention. A number of jurisdictions around the world include in their laws a right to be free from automated decision-making, or an analogous right to contest automated processing of personal data, as well as a right not to be subject to decisions based solely on automation.

For example, Article 22 of the GDPR (General Data Protection Regulation) grants individuals the right not to be subject to automated decision-making, including profiling, except when an automated decision is necessary for a contract; authorized by law; or explicit consent is obtained. Article 22 also contains the caveat that where significant automated decisions are taken on the basis of a legitimate grounds for processing, the data subject still has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Note that Article 21 of the GDPR (General Data Protection Regulation) permits individuals the right to object to any profiling or other processing that is carried out on the basis of legitimate interests or on the basis of a task carried out in the public interest or official authority. [14](#fn14) If a right to object to such processing is exercised, it may continue only if it can be shown that there is a compelling reason to continue the processing that overrides the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

Article 21 also allows the individual the right to object to having their personal information processed for direct marketing purposes, and any related profiling and processing must stop as soon as the objection has been received. [15](#fn15) There are no exemptions or grounds to refuse an individual's objection towards direct marketing.

We support incorporating a circumscribed right to object in PIPEDA (Personal Information Protection and Electronic Documents Act), similar to that found in the GDPR (General Data Protection Regulation).

Currently, Principle 4.3.8 of PIPEDA (Personal Information Protection and Electronic Documents Act) provides that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. We view integrating a right to object and to be free from automated decisions as analogous to the right to withhold consent.

Discussion questions:

1. Should PIPEDA (Personal Information Protection and Electronic Documents Act) include a right to object as framed in this proposal?
2. If so, what should be the relevant parameters and conditions for its application?

Proposal 4: Provide individuals with a right to explanation and increased transparency when they interact with, or are subject to, automated processing

Transparency is a foundational element of PIPEDA (Personal Information Protection and Electronic Documents Act)'s openness principle and a precondition to trust. However, as currently framed, the principle lacks the specificity required to properly address the transparency challenges posed by AI (artificial intelligence) systems, as it does not explicitly provide explanation rights for individuals when interacting with or being subjected to automated processing operations.

The Council of Europe's consultative committee suggests in their *Guidelines on Artificial Intelligence and Data Protection* that: "Data subjects should be informed if they interact with an AI (artificial intelligence) application and have a right to obtain information on the reasoning underlying AI (artificial intelligence) data processing operations applied to them. This should include the consequences of such reasoning." [16](#fn16)

In Europe, there is debate about the interpretation of the GDPR (General Data Protection Regulation) with respect to whether the law requires explanation of system functionality or the rationale for the logic, significance and consequences of specific decisions. [17](#fn17) France and Hungary are among the EU (European Union) Member States that guarantee a right to legibility/explanation about algorithmic decisions in their national data protection legislation. [18](#fn18) For instance, the law in France provides that data subjects have the right to obtain from the controller information about the logic involved in algorithm-based processing. [19](#fn19)

The Government of Canada has expressed its support for algorithmic transparency. [20](#fn20) In its PIPEDA (Personal Information Protection and Electronic Documents Act) white paper, the federal department of Innovation, Science and Economic Development Canada (ISED) proposes amending the law to provide for more meaningful controls and increased transparency to individuals as it relates to AI (artificial intelligence). They suggest that a reformed PIPEDA (Personal Information Protection and Electronic Documents Act) should include "informing individuals about the use of automated decision-making, the factors involved in the decision, and where the decision is impactful, information about the logic upon which the decision is based." [21](#fn21)

We believe the openness principle of PIPEDA (Personal Information Protection and Electronic Documents Act) should include a right to explanation that would provide individuals interacting with AI (artificial intelligence) systems the reasoning underlying any automated processing of their data, and the consequences of such reasoning for their rights and interests. This would also help to satisfy PIPEDA (Personal Information Protection and Electronic Documents Act)'s existing obligations of providing individuals with rights to access and correct their information held by organizations.

In addition to this, we would possibly support enhancing transparency requirements under the law to mandate:

- The conduct and publishing of Privacy Impact Assessments (PIAs), including assessments relating to the impacts of AI (artificial intelligence) processing on privacy and human rights. The published content would be based on a minimum set of requirements that would be developed in consultation with the OPC (Office of the Privacy Commissioner of Canada).
- Public filings for algorithms, similar to U.S. Securities and Exchange Commission filings, with penalties for non-disclosure and non-compliance. Member of Parliament, Nathaniel Erskine-Smith, raised the issue of mandating

filings for algorithms at the Standing Committee on Access to Information, Privacy and Ethics (ETHI). He noted: "if we are serious about that level of transparency and explainability, it could mean a requirement for algorithmic impact assessments in the private sector akin to an SEC filing where non-compliance would come with some sanctions if information is not included." 22 (#fn22)

Discussion questions:

1. What should the right to an explanation entail?
2. Would enhanced transparency measures significantly improve privacy protection, or would more traditional measures suffice, such as audits and other enforcement actions of regulators?

Proposal 5: Require the application of Privacy by Design and Human Rights by Design in all phases of processing, including data collection

Internationally, there are a number of legal and non-binding instruments that instruct organizations to design their products, systems or programs in a manner that avoids possible adverse consequences on privacy, human rights and fundamental freedoms. In its *Guidelines on Artificial Intelligence and Data Protection*, the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data states that:

> *In all phases of the processing, including data collection, AI (artificial intelligence) developers, manufacturers and service providers should adopt a human rights by-design approach and avoid any potential biases, including unintentional or hidden, and the risk of discrimination or other adverse impacts on the human rights and fundamental freedoms of data subjects.* 23 (#fn23)

"Data Protection by Design and by Default" is the meaningful title of Article 25 of the GDPR (General Data Protection Regulation), which applies more broadly than only to AI (artificial intelligence) systems. Article 25 discusses a number of elements of this obligation, including putting in place appropriate technical and organizational measures designed to implement the data protection principles and safeguard individual rights and freedoms. Article 25 further indicates that "an approved certification mechanism" may be used to demonstrate compliance. 24 (#fn24)

The Treasury Board of Canada Secretariat's *Directive on Automated Decision-Making* requires the Government of Canada, before launching into production, to develop processes to test for unintended data biases and other factors that may unfairly impact the outcomes. 25 (#fn25) The *Directive* also requires the completion of an algorithmic impact assessment prior to the production of any automated decision system. The assessment must also be updated when system functionality, or the scope of the Automated Decision System changes in order to continuously monitor for and prevent such negative impacts.

We find each of these texts instructive and respective requirements worthy of incorporation into PIPEDA (Personal Information Protection and Electronic Documents Act).

Discussion questions:

1. Should Privacy by Design be a legal requirement under PIPEDA (Personal Information Protection and Electronic Documents Act)?
2. Would it be feasible or desirable to create an obligation for manufacturers to test AI (artificial intelligence) products and procedures for privacy and human rights impacts as a precondition of access to the market?

Proposal 6: Make compliance with purpose specification and data minimization principles in the AI (artificial intelligence) context both realistic and effective

The Information Technology Association of Canada has conveyed to the ETHI (Standing Committee on Access to Information, Privacy and Ethics) Committee that "having access to broad and vast amounts of data is the key to advancing our artificial intelligence capabilities in Canada." [26] (#fn26) This objective is in tension with the important legal principles of purpose specification and data minimization, which apply to the development and implementation of AI (artificial intelligence) systems under the current PIPEDA (Personal Information Protection and Electronic Documents Act).

It may be difficult to specify purposes that only become apparent after a machine has identified linkages. For example, the Information Accountability Foundation argues that since "the insights data hold are not revealed until the data are analyzed, consent to processing cannot be obtained based on an accurately described purpose." [27] (#fn27) Without being able to identify purposes at the outset, limiting collection to only that which is needed for the purposes identified by the organization, as required by PIPEDA (Personal Information Protection and Electronic Documents Act), is made equally challenging.

Some data protection authorities argue that purpose specification and data minimization are still applicable in the AI (artificial intelligence) context. For example, in discussing data minimization techniques in AI (artificial intelligence) systems, the UK (United Kingdom) Information Commissioner's Office (ICO) notes that "the fact that some data might later in the process be found to be useful for making predictions is not enough to establish its necessity for the purpose in question, nor does it retroactively justify its collection, use or retention." [28] (#fn28) The UK (United Kingdom) ICO (Information Commissioner's Office) further notes that data can also be minimized during the training phase based on the assumption that "not all features included in a dataset will necessarily be relevant to the task." [29] (#fn29) The Norwegian Data Protection Authority suggests that proactively considering data minimization supports the desirable goal of proportionality, which requires consideration of how to achieve the objective of the AI (artificial intelligence) processing in a way that is the least invasive for the individual. [30] (#fn30)

Canadian Parliamentary Committee reporting validates the merits of the principle of data minimization in the context of ethics and AI (artificial intelligence). Specifically, in June 2019, the ETHI (Standing Committee on Access to Information, Privacy and Ethics) Committee recommended that the government modernize Canada's privacy laws and commit "to uphold data minimization, de-identification of all personal information at source when collected for research or similar purpose and clarify the rules of consent regarding the exchange of personal information between government department and agencies." [31] (#fn31)

Purpose specification and data minimization remain complex issues and the potential challenges in adhering to these legal principles in an AI (artificial intelligence) context merit discussing whether there is reason to explore alternative grounds for processing.

Discussion questions:

1. Can the legal principles of purpose specification and data minimization work in an AI (artificial intelligence) context and be designed for at the outset?
2. If yes, would doing so limit potential societal benefits to be gained from use of AI (artificial intelligence)?
3. If no, what are the alternatives or safeguards to consider?

Proposal 7: Include in the law alternative grounds for processing and solutions to protect privacy when obtaining meaningful consent is not practicable

The concept of consent is a central pillar in several data protection laws, including the current PIPEDA (Personal Information Protection and Electronic Documents Act). However, there is evidence that the current consent model may not be viable in all situations, including for certain uses of AI (artificial intelligence). This is in part due to the inability to obtain meaningful consent when organizations are unable to inform individuals of the purposes for which their information is being collected, used or disclosed in sufficient detail so as to ensure they understand what they are being invited to consent to. As noted in our Guidelines on Obtaining Meaningful Consent, clear purpose specification is one of the key elements organizations must emphasize in order to obtain meaningful consent.

In other laws, such as the GDPR (General Data Protection Regulation), consent is only one legal ground for processing among many. [32](#fn32) Alternative grounds for processing under the GDPR (General Data Protection Regulation) include when processing is necessary for the performance of a task carried out in the public interest, and when the processing is necessary for the purposes of the "legitimate interests" pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (in particular where the data subject is a child).

We believe there is a continued role for consent in the use of AI (artificial intelligence) when it can be meaningful, and, to that extent, we would support efforts by the federal government to explore incentivizing new business models that promote innovative consent models. For example, emerging consent technologies and personal information management systems [33](#fn33) offer important opportunities to preserve human agency and meaningfully inform individuals about the development and deployment of AI (artificial intelligence) systems. These approaches should be maximized to facilitate consent whenever possible.

That said, and as outlined in our Report on Consent, [34](#fn34) we acknowledge that alternate grounds to consent may be acceptable in certain circumstances, specifically when obtaining meaningful consent is not practicable and certain preconditions are met. In our Report we proposed that Parliament consider amending PIPEDA (Personal Information Protection and Electronic Documents Act) to introduce new exceptions to consent to allow for socially beneficial activities that the original PIPEDA (Personal Information Protection and Electronic Documents Act) drafters did not envisage. Such alternative grounds would not be intended to relax privacy rules but rather to recognize that consent may not be effective in all circumstances and that more effective measures must be adopted to better protect privacy.

In assessing how a future PIPEDA (Personal Information Protection and Electronic Documents Act) should appropriately deal with consent, particularly in the AI (artificial intelligence) context, we propose that meaningful consent should be required in the first instance for transparency and to preserve human agency. Alternative grounds for processing such as those found in the GDPR (General Data Protection Regulation) and outlined in our Report on Consent should be available in instances where obtaining meaningful consent is not possible and prescribed conditions, such as demonstrating that obtaining consent was considered and impracticable and that a PIA (Privacy Impact Assessment) was conducted and published in advance, are first met.

The use of non-identifiable data, such as through the application of de-identification methods, could also be a factor in determining whether certain other grounds for processing such as legitimate or public interest should be authorized under the Act.

A new consent exception of this nature would necessarily have to be contingent on stronger enforcement powers that would authorize the privacy regulator, where warranted, to assess whether the use of personal information was indeed for broader societal purposes and met the prescribed legal conditions.

Discussion questions:

1. If a new law were to add grounds for processing beyond consent, with privacy protective conditions, should it require organizations to seek to obtain consent in the first place, including through innovative models, before turning to other grounds?
2. Is it fair to consumers to create a system where, through the consent model, they would share the burden of authorizing AI (artificial intelligence) versus one where the law would accept that consent is often not

practical and other forms of protection must be found?

3. Requiring consent implies organizations are able to define purposes for which they intend to use data with sufficient precision for the consent to be meaningful. Are the various purposes inherent in AI (artificial intelligence) processing sufficiently knowable so that they can be clearly explained to an individual at the time of collection in order for meaningful consent to be obtained?
4. Should consent be reserved for situations where purposes are clear and directly relevant to a service, leaving certain situations to be governed by other grounds? In your view, what are the situations that should be governed by other grounds?
5. How should any new grounds for processing in PIPEDA (Personal Information Protection and Electronic Documents Act) be framed: as socially beneficial purposes (where the public interest clearly outweighs privacy incursions) or more broadly, such as the GDPR (General Data Protection Regulation)'s legitimate interests (which includes legitimate commercial interests)?
6. What are your views on adopting incentives that would encourage meaningful consent models for use of personal information for business innovation?

Proposal 8: Establish rules that allow for flexibility in using information that has been rendered non-identifiable, while ensuring there are enhanced measures to protect against re-identification

De-identification is achieved through processes that remove information that can identify individuals from a data set so that the risks of re-identification and disclosure are reduced to low levels. Importantly, however, in fact, there always remains a risk—even if remote—that re-identification may be possible.

There are divergent approaches internationally on whether de-identified information falls within the scope of data protection laws. Many jurisdictions view de-identified or anonymized data as non-personal information falling outside the purview of law. For example, Australia's *Privacy Act 1988* will not apply to information that has undergone de-identification so long as there is no reasonable likelihood of re-identification occurring. [35](#fn35) Similarly, Hong Kong's privacy law will not consider data that is anonymized personal so long as the individuals concerned cannot be directly or indirectly identified. [36](#fn36)

Japan's regime differs substantially in that its *Act on the Protection of Personal Information* applies to the category of "anonymously processed information," and sets out obligations for organizations that anonymize data and/or use anonymized data (including notice). [37](#fn37) Under this Act, consent is not required for use or disclosure of anonymously processed data.

Given there always remains a risk of re-identification, we believe that PIPEDA (Personal Information Protection and Electronic Documents Act) should continue to apply, but that there could be flexibility to use de-identified information (or information rendered non-identifiable) under a new Act. With this flexibility, certain PIPEDA (Personal Information Protection and Electronic Documents Act) principles (such as consent) could either not apply or their application could be relaxed. As mentioned, de-identification could be a factor in deciding whether alternative grounds for processing, such as legitimate interests, should be authorized.

We would also support including in the law penalties for negligence or malicious actions resulting in re-identification of personal information from de-identified datasets. This approach to financial consequences for re-identification is in line with other jurisdictions. For example, Japan's data protection legislation specifically forbids the re-identification of de-identified data with a potential penalty of imprisonment or a fine [38](#fn38) and Australia's proposed *Privacy Amendment (Re-identification Offence) Bill 2016* includes criminal offences and civil penalty provisions for the re-identification of de-identified personal information or the disclosure of such information. [39](#fn39)

Discussion questions:

1. What could be the role of de-identification or other comparable state of the art techniques (synthetic data, differential privacy, etc.) in achieving both legitimate commercial interests and protection of privacy?
2. Which PIPEDA (Personal Information Protection and Electronic Documents Act) principles would be subject to exceptions or relaxation?
3. What could be enhanced measures under a reformed Act to prevent re-identification?

Proposal 9: Require organizations to ensure data and algorithmic traceability, including in relation to datasets, processes and decisions made during the AI (artificial intelligence) system lifecycle

A requirement for algorithmic traceability would facilitate the application of several principles, including accountability, accuracy, transparency, data minimization as well as access and correction. Indeed, several international organizations take the position that being able to trace the source of AI (artificial intelligence) system data is both possible and highly desirable. For example, the OECD (Organisation for Economic Co-operation and Development) *Principles on Artificial Intelligence* state that "AI (artificial intelligence) actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI (artificial intelligence) system lifecycle, to enable analysis of the AI (artificial intelligence) system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art." 40 (#fn40)

The Institute of Electrical and Electronics Engineers (IEEE) notes that:

> *Technologists and corporations must do their ethical due diligence before deploying A/IS [Artificial Intelligence Systems] technology… Similar to a flight data recorder in the field of aviation, algorithmic traceability can provide insights on what computations led to questionable or dangerous behaviors. Even where such processes remain somewhat opaque, technologists should seek indirect means of validating results and detecting harms.* 41 (#fn41)

Several data protection authorities have addressed this issue. For example, the Personal Data Protection Commission of Singapore has recommended implementing both "data lineage" and "data provenance records" in A *Proposed Model Artificial Intelligence Governance Framework*. 42 (#fn42) It explains "data lineage" as "knowing where the data originally came from, how it was collected, curated and moved within the organisation, and how its accuracy is maintained over time. Data lineage can be represented visually to trace how the data moves from its source to its destination, how the data gets transformed along the way, where it interacts with other data, and how the representations change." It explains a "data provenance" record as allowing "an organisation to ascertain the quality of the data based on its origin and subsequent transformation, trace potential sources of errors, update data, and attribute data to their sources."

France's data protection authority (the Commission nationale de l'informatique et des libertés—CNIL), has recommended the development of a "national platform" for algorithmic auditing. 43 (#fn43) This proposal is in line with the proposed *Algorithmic Accountability Act* (AAA), which would give the US Federal Trade Commission (FTC) new powers to require companies to assess their machine learning systems for bias and discrimination. 44 (#fn44) Regulations to be adopted by the FTC (Federal Trade Commission) within two years of the coming into force of the law would require organizations to conduct automated decision impact assessments and data protection impact assessments, "if reasonably possible," in consultation with third parties, including independent auditors and independent technology experts.

Private sector consultancy PwC Australia has also made recommendations about AI (artificial intelligence) governance, taking the position that "AI (artificial intelligence) plans should (…) start with a clear picture of where data has come from, how reliable it is, and any regulatory sensitivities that might apply to its use, before being approved. Data preparation and data 'labelling' processes should be traceable. That is, it should be possible to show an audit trail of everything that has happened to the data over time, in the event that there is a later audit or investigation." 45 (#fn45)

Legal experts Danielle Citron and Frank Pasquale argue that "aggrieved consumers could be guaranteed reasonable notice if scoring systems included audit trails recording the correlations and inferences made algorithmically in the prediction process. With audit trails, individuals would have the means to understand their scores. They could challenge mischaracterizations and erroneous inferences that led to their scores." 46 (#fn46)

As well, ISED (Innovation, Science and Economic Development)'s PIPEDA (Personal Information Protection and Electronic Documents Act) reform paper recommends "Ensuring the accuracy and integrity of information about an individual throughout the chain of custody by requiring organizations to communicate changes or deletion of information to any other organization to whom it has been disclosed." 47 (#fn47)

In considering these expert views and given the importance of being able to trace, analyze and validate AI (artificial intelligence) system outcomes for individuals to be able to avail themselves of existing access and correction rights and also improved human rights protections under a reformed PIPEDA (Personal Information Protection and Electronic Documents Act), we recommend the inclusion of an algorithmic traceability requirement for AI (artificial intelligence) systems.

Discussion question:

1. Is data traceability necessary, in an AI (artificial intelligence) context, to ensure compliance with principles of data accuracy, transparency, access and correction and accountability, or are there other effective ways to achieve meaningful compliance with these principles?

Proposal 10: Mandate demonstrable accountability for the development and implementation of AI (artificial intelligence) processing

Shortcomings with the current framing of the principle of accountability in PIPEDA (Personal Information Protection and Electronic Documents Act) have lead us to conclude that a more robust conception of accountability should be included in a modernized Act. While Principle 4.1 of PIPEDA (Personal Information Protection and Electronic Documents Act) requires organizations to be accountable for the personal information under their control, we propose that the principle be reframed to require "demonstrable" accountability on the part of organizations. Demonstrable accountability would require organizations to be able to provide evidence of adherence with legal requirements on request. The ability for an organization to demonstrate accountability becomes even more important in cases where consent is not required, and organizations are expected to close the protective gap through accountability.

There are a variety of methods by which demonstrable accountability could be achieved, such as requiring traceability, explanation rights, and privacy and human rights impact assessments, as previously discussed. 48 (#fn48) A record keeping requirement would also be necessary to facilitate the OPC (Office of the Privacy Commissioner of Canada)'s ability to conduct proactive inspections. Such inspection powers currently exist in the UK (United Kingdom) and several other countries globally and are an essential mechanism for effective enforcement in favour of protecting rights and preventing harms. As the International Technology Law Association's *Responsible AI (artificial intelligence): a Global Policy Framework* explains, "beneficial AI (artificial intelligence) demands human accountability. General principles, even if well intended, are useless without enforceable accountability regimes and without efficient governance models." 49 (#fn49)

The Privacy Commissioner has the authority under section 37 of the *Privacy Act* to carry out investigations at his discretion in order to ensure a government institution is compliant with specific sections of the Act. The addition of such a provision in PIPEDA (Personal Information Protection and Electronic Documents Act), where the OPC (Office of the Privacy Commissioner of Canada) could proactively inspect the practices of organizations, would move the law towards a model of demonstrable accountability.

We propose that the law also require independent third-party auditing throughout the lifecycle of the AI (artificial intelligence) system. Auditors could be subject to financial penalties if they act negligently by signing off on practices that are in fact not compliant.

We would also favour introducing into PIPEDA (Personal Information Protection and Electronic Documents Act) incentives for organizations adopting demonstrable accountability measures, such as giving consideration of these measures as mitigating factors during an investigation, or the imposition of financial penalties for non-compliance.

Finally, we are of the view that true accountability should lead to liability for humans, not machines. As such, demonstrable accountability should be strongly linked with fault-finding and liability for design failures that lead to privacy incursions. The International Technology Law Association's *Responsible AI (artificial intelligence): a Global Policy Framework* aptly captures why humans must remain responsible:

> *even if AI (artificial intelligence) might force us to reconsider the accountability of certain actors, it should be done in a way that shifts liability to other human actors and not to the AI (artificial intelligence) systems themselves (…) Holding AI (artificial intelligence) systems directly liable runs the risk of shielding human actors from responsibility and reducing the incentives to develop and use AI (artificial intelligence) responsibly.* 50 (#fn50)

Discussion questions:

1. Would enhanced measures such as those as we propose (record-keeping, third party audits, proactive inspections by the OPC (Office of the Privacy Commissioner of Canada)) be effective means to ensure demonstrable accountability on the part of organizations?
2. What are the implementation considerations for the various measures identified?
3. What additional measures should be put in place to ensure that humans remain accountable for AI (artificial intelligence) decisions?

Proposal 11: Empower the OPC (Office of the Privacy Commissioner of Canada) to issue binding orders and financial penalties to organizations for non-compliance with the law

The significant risks posed to privacy and human rights by AI (artificial intelligence) systems demand a proportionally strong regulatory regime. To incentivize compliance with the law, PIPEDA (Personal Information Protection and Electronic Documents Act) must provide for meaningful enforcement with real consequences for organizations found to be non-compliant.

The need to legislate for stronger enforcement as a privacy protective measure in the digital age was echoed in the Council of Europe's 2017 *Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) and Possible Regulatory Implications*, which advised that "privacy, as the exercise of other human rights, requires effective enforcement." 51 (#fn51)

Canada's privacy laws have unfortunately fallen significantly behind those of trading partners in terms of the enforcement. At the same time, most Canadians believe their privacy rights are not respected by organizations. Such a sentiment is not conducive to building consumer trust, and is undesirable from both an individual and organizational perspective. The law should provide for enforcement mechanisms that ensure individuals have access to a quick and effective remedy for the protection of their privacy rights, and that create incentives for broad compliance by commercial organizations.

Among the improvements required to PIPEDA (Personal Information Protection and Electronic Documents Act) is to empower the Privacy Commissioner of Canada to make binding orders and impose consequential penalties for non-compliance with the law. Giving these powers to a first level authority rather than requiring individuals to wait until a court, several years after an alleged violation, upholds a complaint, is a much more effective way to ensure the timely enjoyment of rights.

In other jurisdictions within Canada and abroad, privacy and data protection regulators have the authority to issue binding orders and impose financial penalties. The range of order making powers includes the ability to require an organization to stop collecting, using or disclosing personal information, to destroy personal information collected in contravention of the legislation, and more generally to order the application of such remedial measures as are appropriate to ensure the protection of the personal information, among others. Regarding financial penalties, in Europe, for example, the GDPR (General Data Protection Regulation) allows for the issuance of "administrative fines". Organizations in breach of the GDPR (General Data Protection Regulation) can be fined up to 4% of annual global turnover or € (Euros)20 Million (whichever is greater).

True order-making powers and financial penalties would lead to quicker resolutions for Canadians and provide them with reassurance to be able to confidently participate in the digital marketplace. Ultimately, enforcement mechanisms should result in quick and effective remedies for individuals, and broad and ongoing compliance by organizations and institutions. Without effective enforcement, rights become hollow and trust dissipates.

Discussion questions:

1. Do you agree that in order for AI (artificial intelligence) to be implemented in respect of privacy and human rights, organizations need to be subject to enforceable penalties for non-compliance with the law?
2. Are there additional or alternative measures that could achieve the same objectives?

Footnotes

1 G20 Ministerial Statement on Trade and Digital Economy, June 2019.

2 Canada's AI (artificial intelligence) Imperative: Overcoming risks, building trust, Deloitte, 2019, p. (page)20.

3 Centre for Information Policy Leadership, *First Report: Artificial Intelligence and Data Protection in Tension*, Oct 2018, pg. (pages) 12-13. The Office of the Victorian Information Commissioner, Artificial Intelligence and Privacy, 2018.

4 The Office of the Victorian Information Commissioner, Artificial Intelligence and Privacy, 2018. See blog post from lawyer, Doug Garnett, *AI (artificial intelligence) & Big Data Question: What happened to the distinction between primary and secondary research?* Mar 22 2019.

5 The Office of the Victorian Information Commissioner, Artificial Intelligence and Privacy, 2018.

6 Ian Kerr, "Robots and Artificial Intelligence in Health Care," *Canadian Health Law and Policy*, 5th edition, 2017, p. (page)279.

7 See OECD (Organisation for Economic Co-operation and Development) Principles on Artificial Intelligence, May 21, 2019; and, the OECD (Organisation for Economic Co-operation and Development)'s press release: Forty-two countries adopt new OECD (Organisation for Economic Co-operation and Development) Principles on Artificial Intelligence, May 22, 2019.

8 Institute of Electrical and Electronics Engineers (IEEE)'s Global Initiative on Ethics of Autonomous and Intelligence Systems' report *Ethically Aligned Design*, First Edition, 2019, p. (page)16.

9 UK (United Kingdom) ICO (Information Commissioner's Office) guidance, *Big data, artificial intelligence, machine learning and data protection*, 2017.

10 Paul Nemitz, "Constitutional democracy and technology in the age of artificial intelligence," *Philosophical Transactions A*, October 15, 2018.

11 2019 Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners.

12 ICDPPC (International Conference of Data Protection and Privacy Commissioners)'s 2018 Declaration on Ethics and Data Protection in Artificial Intelligence, adopted in Brussels. Please note that the ICDPPC (International Conference of Data Protection and Privacy Commissioners) has been renamed the Global Privacy Assembly.

13 ICDPPC (International Conference of Data Protection and Privacy Commissioners)'s 2019 International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights, adopted in Tirana, Albania

14 Refer to Article 21 of the GDPR (General Data Protection Regulation), and see the UK (United Kingdom) ICO (Information Commissioner's Office)'s guidance, *What if Article 22 doesn't apply to our processing?* Retrieved 13 Nov 2019

15 *Ibid.*

16 Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, *Guidelines on Artificial Intelligence and Data Protection*, January 25, 2019, section II(11).

17 Discussion by Jake Goldenfein in a report by the Victorian Information Commissioner, "Closer to the Machine: Technical, Social and Legal Aspects of AI (artificial intelligence)," 2019, p. (page)49.

18 For more analysis see: Malgieri, G. (2019). "Automated decision-making in the EU (European Union) Member States: The right to explanation and other "suitable safeguards" in the national legislations." *Computer Law & Security Review* 35: 5.

19 See, France's Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Also refer to the CNIL (Commission nationale de l'informatique et des libertés) report, How Can Humans Keep the Upper Hand? Ethical Matters Raised by Algorithms and Artificial Intelligence (Dec 2017); and, Malgieri, G. (2019). "Automated decision-making in the EU (European Union) Member States: The right to explanation and other "suitable safeguards" in the national legislations." *Computer Law & Security Review* 35: 5.

20 The Standing Committee On Access To Information, Privacy And Ethics, June 19, 2018.

21 Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act*, May 2019.

22 The Standing Committee on Access to Information, Privacy and Ethics (ETHI), Evidence (42-1), No. 145, Apr 30 2019.

23 Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, Guidelines on Artificial Intelligence and Data Protection, January 25, 2019, section II(3).

24 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, (GDPR).

25 TBS *Directive on Automated Decision-Making*, April 19, 2019.

26 Testimony by André Leduc (Vice-President, Government Relations and Policy, Information Technology Association of Canada) before the Standing Committee on Access to Information, Privacy and Ethics, June 6, 2019.

27 Advanced Data Analytic Processing – 2019 An Update, The Information Accountability Foundation, p. (page)14, footnote 26.

28 UK (United Kingdom) Information Commissioner's Office, "Data minimisation and privacy-preserving techniques in AI (artificial intelligence) systems," (blog) August 21, 2019.

29 *Ibid*.

30 Norwegian Data Protection Authority, *Artificial Intelligence and Privacy*, January 2018.

31 Privacy and Digital Government Services, Report of the Standing Committee on Access to Information, Privacy and Ethics, June 2019.

32 Regulation (EU (European Union)) 2016/679 (General Data Protection Regulation), Article 6(1)(f).

33 European Data Protection Supervisor (EDPS), Opinion 9/2016, EDPS (European Data Protection Supervisor) Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data. October 26, 2016.

34 Office of the Privacy Commissioner of Canada, Report on Consent, 2017.

35 Refer to the Office of the Australian Information Commissioner's "De-Identification and the Privacy Act" (p. (page) 3).

36 Refer to the Office of the Privacy Commissioner for Personal Data, Hong Kong's "Guidance on Personal Data Erasure and Anonymisation" (p. (page)4).

37 Japan's *Act on the Protection of Personal Information*, English version.

38 *Ibid*, article 84.

39 Status on the Parliamentary site as of November 29, 2019: "Lapsed at the end of Parliament," July 2019.

40 OECD (Organisation for Economic Co-operation and Development) Principles on Artificial Intelligence, May 21, 2019.

41 Institute of Electrical and Electronics Engineers (IEEE)'s Global Initiative on Ethics of Autonomous and Intelligence Systems' report *Ethically Aligned Design*, First Edition, 2019, p. (page)132.

42 A Proposed Model Artificial Intelligence Governance Framework

43 CNIL (Commission nationale de l'informatique et des libertés), How Can Humans Keep the Upper Hand? Ethical Matters Raised by Algorithms and Artificial Intelligence, December 2017.

44 Refer to the *Algorithmic Accountability Act*, introduced by Democratic lawmakers in the U.S. House of Representatives and the U.S. Senate in April 2019, and as discussed by McCarthy Tétrault in "US Lawmakers propose US Algorithmic Accountability Act intended to regulate AI (artificial intelligence)," April 22, 2019.

45 PwC Australia, *Digital Pulse*: "Three governance considerations to unlock the potential of AI (artificial intelligence)," July 11, 2019.

46 Frank Pasquale and Danielle Citron, "The Scored Society: Due Process for Automated Predictions," *Washington Law Review*, Vol. 89, 2014, University of Maryland Francis King Carey School of Law, Legal Studies Research Paper, No. 2014 – 8, p. (page)28.

47 Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act*, May 2019.

48 Mark Latonero, *Governing Artificial Intelligence: Upholding Human Rights & Dignity*, Data & Society, 2018.

49 The International Technology Law Association's *Responsible AI (artificial intelligence): a Global Policy Framework*, May 23, 2019, p. (page)96.

50 The International Technology Law Association's *Responsible AI (artificial intelligence): a Global Policy Framework*, May 23, 2019, p. (page)81.

51 Committee of Experts on Internet Intermediaries, Council of Europe "Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications." DGI (2017)12, March 2018, p. (page)34

Date modified:

2020-01-28